Table of Contents

1. What if the Certification Authorities won't accept my IP addresses or domain name?

Question: A prospective offeror has attempted to procure the required ACES certificates. They have Static IP Addresses xxx.xx.xx.xxx and xxx.xx.xx.xxx.. However neither DST nor ORC will accept these as valid IP Addresses. This company has formed from several mergers and can demonstrate that they have acquired the rights to the NetRange that includes these two IP addresses. They believe that DST and ORC want only host names such as <current_corporate_name>.com. The prospective offeror claims to neither need nor want in-coming access to these PCs and that they will only be used to access the Networx Hosting Center. Do you [the Government] have contacts at DST or ORC that we can discuss this issue? Any other suggestions?

Answer: The DST and/or ORC help desk has already resolved this issue. Generally, however, we would expect that the Distinguished Name (DN) be a hostname which is assigned to the machine and within a domain under the potential offeror's control. Giving a machine a hostname does not imply that it will allow in-coming access; that is relegated and enforced by the software/firewall configuration on the machine. It is also not specifically required that a hostname which is used in a DN be resolvable externally provided it is under a domain controlled by the potential offeror and that it is acknowledged by the controller of the domain as listed in the Internet whois database.

2. Do I need information from the Government to complete the PKCS #10 request?

Question: A prospective offeror has attempted to procure the required ACES certificates. They indicated that they were informed by one of the ACES Help desks that the field "PKCS #10 Request" needs to have specific information that is to be provided to the vendor by the Government. Their question involved the means of obtaining this information from the Government.

Answer: The PKCS #10 file must be generated by the potential offeror. The PKCS #10 file generation does require information (Country, State, City, Distinguished Name, etc). There is no unique information required to generate the PKCS #10 file that must be supplied by GSA. There are multiple different tools which can be used to generate a PKCS #10 file including MyCert, a Windows-based utility which is mentioned in the instructions; OpenSSL, a Unix/Windows utility which is used by MyCert but can also be used stand-alone; GNU TLS, a Unix utility which includes a program called certtool. We have tested with MyCert and OpenSSL (stand-alone).

3. Where can I find the Government-prepared mycert.ini file?

The Windows utility (http://mycert.pavelec.net/) includes an initialization file called "mycert.ini." The following version of the mycert.ini file has been modified for the Networx application. This file may be used in place of the ".ini" file on the My Certificate Wizard web site. Users are expected to be familiar with the PKCS #10 process and the mycert.ini file. The Government assumes no liability should the offerer elect to use this or any other source to generate the component certificate request.

```
# The configuration file for My Certificate Wizard (mycert.exe)
# ============================================================
#
# My Certificate Wizard is a simple Win32 application used to simplify
# the process of creating the PKCS#10 certificate request and private
# key for the common user.
#
```

```
# The openssl dynamic loadable library (DLL) must be accessible: libeay32.dll.
# This file usually comes with the software the user creates the keys for...
#
# The input text restrictions applied by this program is not intended to defeat
# the experienced user. The primary goal is to help conduct the boring act
# as smoothly as possible.
#
# It is expected the CA/service admin prepares this INI file
# for his/her users then the EXE and INI files are bundled with
# the other application software and sent to the users.
#
# The program does not contain much of descriptive texts, anyway
# the administrator should equip the users with the suitable reference
# manual so they will have a clue of what this damned thing should do.
#
# Most of the mycert features are reflected in this file's comments.
#
# Notes on building: If you get the source and want to rebuild the program,
# you'll need the MinGW/MSYS environment (http://www.mingw.org) for Win32
# and the OpenSSL includes (http://www.openssl.org) in addition.
# These tools are free.
#
# Hopefully My Certificate Wizard will be usable for the power users too.
# Have fun like I had while I was coding this.
#
# Vlada Macek, Oct 2004
# Contact: mycert a seznam d cz
# Bug reports, patches, ideas, opinions and thankyou mail is welcome!
#
# ---
#
# This conf file must reside in the same folder as the wizard's EXE, must have
# the same name and must have the INI extension. Alternatively: The path to
# the INI file may be forced by the mycert.exe's first command line argument.
# If this parameter does not contain a full path to the file, the system
# searches for the file in the Windows directory (such searching is then
# not reported by mycert).
#
# $Id: mycert.ini,v 1.8 2004/11/09 09:02:44 tuttle Exp $

[dn]

# The default values of the Distinguished Name of the user.
# C is Country, ST is State, L is Locality, O is Org. and OU is Org. Unit.
# The *_allow truth values specify whether such field will be editable.
# The default is yes.
#
# This way the really simple form for creating custom DN can be created.
#

C=US
C_allow=0
ST=null
ST_allow=0
```

```
L=null
L_allow=0
O=
O_allow=1
OU=
OU_allow=1

# These may also be set as default values:
#
### CN=<Fully Qualified Domain Name>
### emailAddress=<Administrators Email Address>


## --- POSIX Regular Expressions ---

# With the following options you can restrict the user input in the
# very flexible way. Syntax is Extended Posix RE, case sensitive.
# See http://en.wikipedia.org/wiki/Regular_expression,
# GNU Regular Expression Library docs and other resources on the web.
#
# WARNING: These work only in case the Regular Expression checking was
# enabled while compiling My Certificate Wizard. Furthermore, the field
# is regexp checked only in case it's user editation was not disallowed
# by above *_allow options.

# Example: "Full Name, Company" (full name - two or three ASCII words not shorter
#          than 2 characters, `-' and `.' are allowed in them)
# CN_re=^([-.[:alpha:]]{2,}[[:space:]]){1,2}[-.[:alpha:]]{2,}, [Cc]ompany$

#CN_re=
#email_re=^[[:graph:]]+@[[:graph:]]+$
#C_re=
#ST_re=
#L_re=
#O_re=
#OU_re=


[paths]

# Specification of the default output folder. Two files are to be created here.
# <CN>.key and <CN>.req, where <CN> is the Common Name given by the user.
# The output folder may be changed by the user in the dialog box.
# Default: dir=C:\

dir=C:\

[openssl]

# Most of the following options define behaviour of the underlying
# openssl engine that is responsible for creating the private key
# and the request.
#
# For full option description see OpenSSL's man page (man req)
```

```
# http://www.openssl.org/docs/apps/req.html
#

# Option conforming to the OpenSSL req -nodes ("No DES" encryption) option.
# If this is set to 1, the pass phrase input lines will be inactive.
# Be warned last time now before you let your users to create unprotected keys.
# Default: nodes=0

# An option enforcing input of the passphrase.
# If it is > 0, it specifies the enforced passphrase minimum length.
# If it is = 0 and user enters passphrase shorter than 4 chars,
# he/she will still be warned that it is insecure.
# The nodes= option above takes precedence over this one.
# Default: minpass=0
minpass=6

# Option conforming to the OpenSSL req -newkey option.
# Default: keytype=rsa:1024
keytype=rsa:1024

# Option conforming to the OpenSSL req -outform option.
# Default: outformat=PEM

# Option conforming to the OpenSSL req -keyform option.
# Default: keyformat=PEM

# Option conforming to the OpenSSL req -pubkey option.
# Default: pubkey=0

# Option conforming to the OpenSSL req -noout option.
# Default: norequest=0

# Option conforming to the OpenSSL req -asn1-kludge option.
# Default: asn1kludge=0

# Option conforming to the OpenSSL req -[md5|sha1|md2|mdc2] options.
# Default: digest=sha1


[openvpn]

# If you're not using OpenVPN software (http://openvpn.sourceforge.net),
# please ignore this section.
#
# The following option let you specify the path to the OpenVPN configuration
# file template. If given, the following actions will be taken when you're
# creating the private key and the request:
#
#           - template file will be copied to the output folder
#           - it will be named the same way as the key/req files + .OVPN extension
#           - 'key' and 'cert' options will be appended at the end with the correct
#             path to the key file.
#
# The user should be instructed (in his friendly VPN documentation written
```

```
# by his friendly admin) to store the certificate file (retrieved later
# from the CA) to the right folder.
# Default: Feature is off.
# Example: template=C:\mycert\template_ovpn.txt


[extensions]

# Here it is possible to redefine the private key filename extension.
# Default: key=key

# Here it is possible to redefine the certificate request filename extension.
# Default: req=req

# Here it is possible to redefine the certificate filename extension.
# Default: cert=cert

# Here it is possible to redefine the OpenVPN configuration filename extension.
# Ignore this option if you don't use the template= option above.
# Default: ovpn=ovpn


[strings]

# Dynamic retranslation of strings shown to user. Could serve as a localization
# engine as well as the way of how the messages and labels could be customized
# for the particular use of the program.
#
# Important: The caret sign (^) means newline. On the right side there must be
# the same number of carets as is on the left side. The counts of the formatting
# signs (%) on the left and right sides are also compared as a trivial check for
# typos. Maintain the same structure of the message. Don't use excessive
# whitespace around messages. The ampersand (&) denotes the hotkey character
# for the dialog item. It's up to you to design these hotkeys in the dialogs.
#

# This is the user information feature. Text assigned to the option will be
# displayed in the Message box right before the main dialog. So you could
# inform the user exactly about what do you want from him/her. E.g. about
# the format of the Common name. Carets (^) are transformed to newlines.
#manifesto=blah^blah

# This is the caption of the previous Message box window.
# Welcome= Test


## --- Main Dialogs ---

My Certificate Wizard=ACES VPN IPSec PKCS#10 Request Generator
Distinguished Name=User Inputs
&Common Name (eg. your name):=Host Name (FQDN)
&E-mail Address:= Administrator's Email Address
# C&ountry Name (2 letters):=
&State or Province (full name):= " "
```

&Locality Name (eg. city):= " "
Organization &Name (eg. company):= Company Name or Orgaization
Organizational &Unit Name (eg. section):= Department or Agency
Private Key Protection=" "
&Pass phrase:= Private Key password
Pass phrase (&again):= Private Key password (again)

Output=
Output &Folder:=
Chan&ge...=
Create &Request=
Cancel=

#Generating your private key and the request.^Please wait.=

#My Certificate Wizard - Request=
#Status=
#Done. The following files were created in the output folder:=
#- %s.%s (Private key)^- %s.%s (Certificate request)^- %s.%s (OpenVPN configuration)=
#- %s.%s (Private key)^- %s.%s (Certificate request)=
#Please keep your private key file protected! Do not transmit it elsewhere.=
#Your request=
#Copy the following certificate &request and send it to your Certificate Authority (CA):=
#&Quit=
#&Copy to clipboard=

--- About ---

#Version %s=
#About= About
#My Certificate Wizard^Version %s^^http://www.sweb.cz/mycert^^(c) 2004 Vlada Macek^Released under the terms of GNU General Public License.^http://www.gnu.org^^The development was funded by Hieronymus,^translation and software localization company.^http://www.hiero.cz/us=

--- Message Boxes ---

#Please select the folder where your new private key and request shall be saved:=
#Your two passphrases do not match!=
#The following lines were added by the My Certificate Wizard.=

#Input Error=
#Common Name must not be blank!=

#Confirmation=
#Some files named %s.* already exist in the output folder! Once they are lost, it may be hard to get them back.^Are you sure to OVERWRITE them?=

#Security Restriction=
#Your passphrase must be at least %d characters long. %d is not enough!=

#Security Warning=

#Warning: You've entered no passphrase. Do you really want to leave your private key UNENCRYPTED?=
#Your passphrase is really short (under %d characters). Are you sure to use such weak protection?=

#Configuration Glitch=
#The INI file disables creating both the certificate request and the public key. So no reasonable output will be given.^This is probably not what you want.=

#Configuration Error=
#Error finding OpenVPN input template file: %s^No OpenVPN configuration could be created.=

#Fatal Error=
#Function %s failed with error %d: %s=

#Filename: %s=
#(Cannot read the file.)=
#Failure copying files=
#Unable to copy '%s' to '%s' - error %d=
#Warning=

--- Regular expression matching ---

The following lines are used only in case the Regular Expression
checking was enabled while compiling My Certificate Wizard.

#Regular expression error=
#Cursor will be moved to the field that^appears to be in an unallowed form.^Please correct your input.=
#Cursor will be moved to the field for which the regular expression^compilation have failed with the following error:^%s=
#Cursor will be moved to the field for which the regular expression^matching have failed with the following error:^%s=

--- OpenSSL errors ---

#OpenSSL Error=
#Unknown digest name.=
#Could not read specified parameter file.=
#Unable to load DSA parameters from file.=
#Could not get the public key.=
#Certificate does not contain DSA parameters.=
#Could not initialize output file.=
#Private key is too short.=
#Could not allocate the private key.=
#Problem generating RSA key.=
#Problem generating DSA key.=
#Error: Private key is blank.=
#Error assigning private output filename.=
#Could not write the private key.=
#Problem allocating request.=
#Problems generating certificate request. Please check your input.^(Hint: No field in the Distinguished Name section may be blank.)=
#Problem signing certificate request.=

```
#Problems assigning the output filename.=
#Error getting public key.=
#Bad output format specified.=
#Unable to write X509 request.=


# END mycert.ini -- The configuration file for My Certificate Wizard (mycert.exe)
# ============================================================
```